Optimal discrimination of quantum operations

Massimiliano F. Sacchi
QUIT, Unità INFM and Dipartimento di Fisica "A. Volta", Università di Pavia, I-27100 Pavia, Italy.
(Dated: February 1, 2008)

We address the problem of discriminating with minimal error probability two given quantum operations. We show that the use of entangled input states generally improves the discrimination. For Pauli channels we provide a complete comparison of the optimal strategies where either entangled or unentangled input states are used.

arXiv:quant-ph/0505183v1 24 May 2005

Quantum nonorthogonality is a basic feature of quantum mechanics that has deep implications in many areas, as quantum computation and communication, quantum entanglement, cloning, and cryptography. Nonorthogonality is strongly related to the concept of distinguishability, and many measures have been defined to compare quantum states [1] and quantum processes [2], according to some experimentally or theoretically meaningful criteria. Since the pioneering work of Helstrom [3] on quantum hypothesis testing, the problem of discriminating nonorthogonal quantum states has received a lot of attention [4], with some experimental verifications as well [5]. The most popular scenarios are the minimal-error probability discrimination, where each measurement outcome selects one of the possible states and the error probability is minimized, and the optimal unambiguous discrimination [6], where unambiguity is paid by the possibility of getting inconclusive results from the measurement. Stimulated by the rapid developments in quantum information theory, the problem of discrimination has been addressed also for bipartite quantum states, along with the comparison of global strategies where unlimited kind of measurements is considered, with the scenario of LOCC scheme, where only local measurements and classical communication are allowed [7].

The concepts of nonorthogonality and distinguishability can be applied also to quantum operations, namely all physically allowed transformations of quantum states. Not very much work, however, has been devoted to the problem of discriminating general quantum operations, and major efforts have been directed at the case of unitary transformations [8]. In fact, the most elementary formulation of the problem can be recast to the evaluation of the norm of complete boundedness [9], which is in general a very hard task. We recall that such a norm entered the quantum information field as the diamond norm [10], and one of its most relevant application is found in the problem of quantifying quantum capacities of quantum information channels [11].

In this Letter, we address the problem of discriminating with minimal error probability two given quantum operations. After briefly reviewing the case of quantum states, we formulate the problem for two quantum operations. Differently from the case of unitary transformations [8], we show that entangled input states generally improve the discrimination. We prove that the use of an arbitrary maximally entangled state turns out to be always an optimal input when we are asked to discriminate two quantum operations that generalize the Pauli channel in any dimension. In the case of qubits, we give a complete comparison of the strategies where either entangled or unentangled states are used at the input of the Pauli channels, thus characterizing the channels where entanglement is really useful to achieve the ultimate minimal error probability in the discrimination.

In the problem of discrimination two quantum states ρ_1 and ρ_2, given with a priori probability p_1 and $p_2 = 1-p_1$, respectively, one has to look for the two-values POVM $\{\Pi_i \geq 0\,,\, i=1,2\}$ with $\Pi_1 + \Pi_2 = I$ that minimizes the error probability

$$p_E = p_1 \mathrm{Tr}[\rho_1 \Pi_2] + p_2 \mathrm{Tr}[\rho_2 \Pi_1]\ . \tag{1}$$

We can rewrite

$$\begin{aligned} p_E &= p_1 - \mathrm{Tr}[(p_1\rho_1 - p_2\rho_2)\Pi_1] \\ &= p_2 + \mathrm{Tr}[(p_1\rho_1 - p_2\rho_2)\Pi_2] \\ &= \frac{1}{2}\left\{1 - \mathrm{Tr}[(p_1\rho_1 - p_2\rho_2)(\Pi_1 - \Pi_2)]\right\}\ , \end{aligned} \tag{2}$$

where the third line can be obtained by summing and dividing the two lines above. The minimal error probability can then be achieved by taking the orthogonal POVM made by the projectors on the support of the positive and negative part of the Hermitian operator $p_1\rho_1 - p_2\rho_2$, and hence one has

$$p_E = \frac{1}{2}\left(1 - \|p_1\rho_1 - p_2\rho_2\|_1\right)\ , \tag{3}$$

where $\|A\|_1$ denotes the trace norm of A. Equivalent expressions for the trace norm are the following

$$\|A\|_1 = \mathrm{Tr}\sqrt{A^\dagger A} = \max_U |\mathrm{Tr}[UA]| = \sum_i s_i(A)\ , \tag{4}$$

where the maximum is taken over all unitary operators, and $\{s_i(A)\}$ denote the singular values of A. In the case of Eq. (3), since the operator inside the norm is Hermitian, the singular values just corresponds to the absolute value of the eigenvalues.

The problem of optimally discriminating two quantum operations $\mathcal{E}_1$ and $\mathcal{E}_2$ can be reformulated into the problem of finding in the input Hilbert space $\mathcal{H}$ the state ρ

such that the error probability in the discrimination of the output states $\mathcal{E}_1(\rho)$ and $\mathcal{E}_2(\rho)$ is minimal. We are interested in the possibility of exploiting entanglement in order to increase the distinguishability of the output states. In this case the output states to be discriminated will be of the form $(\mathcal{E}_1 \otimes \mathcal{I}_\mathcal{K})\rho$ and $(\mathcal{E}_2 \otimes \mathcal{I}_\mathcal{K})\rho$, where the input ρ is generally a bipartite state of $\mathcal{H} \otimes \mathcal{K}$, and the quantum operations act just on the first party whereas the identity map $\mathcal{I} = \mathcal{I}_\mathcal{K}$ acts on the second.

In the following we will denote with p'_E the minimal error probability when a strategy with unentangled input is adopted. Hence, without the use of entanglement the minimal error probability is given by

$$p'_E = \frac{1}{2}\left(1 - \max_{\rho\in\mathcal{H}} \|p_1\mathcal{E}_1(\rho) - p_2\mathcal{E}_2(\rho)\|_1\right) , \qquad (5)$$

whereas, by allowing the use of entangled input states, one has

$$p_E = \frac{1}{2}\left(1 - \max_{\rho\in\mathcal{H}\otimes\mathcal{K}} \|p_1(\mathcal{E}_1\otimes\mathcal{I})\rho - p_2(\mathcal{E}_2\otimes\mathcal{I})\rho\|_1\right) . \qquad (6)$$

The maximum of the trace norm in Eq. (6) is equivalent to the norm of complete boundedness [9], and in fact for finite-dimensional Hilbert space one can just consider $\mathcal{K} = \mathcal{H}$ [9, 10].

From the linearity of quantum operations, the following property of the trace norm [12]

$$\|aA + (1-a)B\|_1 \le a\|A\|_1 + (1-a)\|B\|_1 \qquad (7)$$

with $0 \le a \le 1$, and the convexity of the set of states, it follows that in both Eqs. (5) and (6) the maximum is achieved by pure states.

The use of entanglement generally improves the discrimination, and such an improvement can be very remarkable when increasing the dimension of the Hilbert space. Consider for example the situation where one has to discriminate between the identity map and the completely depolarizing map, with $\dim(\mathcal{H}) = d$. One has

$$\begin{aligned}
&\mathcal{E}_1(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi| \qquad |\psi\rangle \in \mathcal{H} ,\\
&\mathcal{E}_2(|\psi\rangle\langle\psi|) = \frac{I}{d} \qquad |\psi\rangle \in \mathcal{H} ,\\
&(\mathcal{E}_1\otimes\mathcal{I})(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi| \qquad |\psi\rangle \in \mathcal{H}\otimes\mathcal{H} ,\\
&(\mathcal{E}_2\otimes\mathcal{I})(|\psi\rangle\langle\psi|) = \frac{I}{d}\otimes \mathrm{Tr}_1[|\psi\rangle\langle\psi|] \qquad |\psi\rangle \in \mathcal{H}\otimes\mathcal{H} ,
\end{aligned}$$

where I denotes the identity matrix, and Tr_i denotes the partial trace with respect to the ith Hilbert space.

Without the use of entanglement, one has

$$\begin{aligned}
p'_E &= \frac{1}{2}\left(1 - \max_{|\psi\rangle}\left\|p_1|\psi\rangle\langle\psi| - p_2\frac{I}{d}\right\|_1\right)\\
&= \frac{1}{2}\left[1 - \left(\left|p_1 - \frac{p_2}{d}\right| + p_2\frac{d-1}{d}\right)\right] , \qquad (8)
\end{aligned}$$

whereas, by considering an input maximally entangled state $|\phi\rangle$, one obtains the bound

$$\begin{aligned}
p_E &\le \frac{1}{2}\left(1 - \left\|p_1|\phi\rangle\langle\phi| - p_2\frac{I\otimes I}{d^2}\right\|_1\right)\\
&= \frac{1}{2}\left[1 - \left(\left|p_1 - \frac{p_2}{d^2}\right| + p_2\frac{d^2-1}{d^2}\right)\right] . \qquad (9)
\end{aligned}$$

For $p_1 = p_2 = 1/2$, e.g., one has $p'_E = \frac{1}{2d}$ and $p_E \le \frac{1}{2d^2}$ [indeed, from what follows, one has equality in Eq. (9) for any maximally entangled input state].

On the other hand, there are situations in which entanglement is not needed to achieve the ultimate minimal error probability, as in the case of discrimination between two unitary transformations [8].

Any quantum operation $\mathcal{E}$ is a completely positive map, and hence can be written in the Kraus form [13]

$$\mathcal{E}(\rho) = \sum_n K_n\rho K_n^\dagger , \qquad (10)$$

where K_n are operators on the Hilbert space $\mathcal{H}$ of the quantum system (here on, for simplicity, we consider operations that map states from $\mathcal{H}$ to $\mathcal{H}$), and satisfy the completeness relation $\sum_n K_n^\dagger K_n = I$, thus preserving the trace of ρ.

Using the notation of Ref. [14] for bipartite vectors

$$\begin{aligned}
|A\rangle\!\rangle &\equiv \sum_{n,m}\langle n|A|m\rangle\, |n\rangle\otimes|m\rangle\\
&= A\otimes I|I\rangle\!\rangle = I\otimes A^\tau|I\rangle\!\rangle , \qquad (11)
\end{aligned}$$

one can write the evolution under $\mathcal{E}\otimes\mathcal{I}$ of a pure bipartite state $\rho = |\xi\rangle\!\rangle\langle\!\langle\xi|$ (with $\mathrm{Tr}[\rho] = \mathrm{Tr}[\xi^\dagger\xi] = 1$) as follows

$$(\mathcal{E}\otimes\mathcal{I})|\xi\rangle\!\rangle\langle\!\langle\xi| = (I\otimes\xi^\tau)\sum_n |K_n\rangle\!\rangle\langle\!\langle K_n|\,(I\otimes\xi^*) , \qquad (12)$$

where τ and $*$ denote transposition and complex conjugation on the basis chosen in Eq. (11). Then, the minimal error probability in Eq. (6) rewrites

$$p_E = \frac{1}{2}\left(1 - \max_{\mathrm{Tr}[\xi^\dagger\xi]=1}\|I\otimes\xi^\tau\Delta I\otimes\xi^*\|_1\right) , \qquad (13)$$

where Δ is Hermitian, and in terms of the Kraus operators $\{K_n^{(1)}\}$ and $\{K_m^{(2)}\}$ of the quantum operations is given by

$$\Delta = p_1\sum_n |K_n^{(1)}\rangle\!\rangle\langle\!\langle K_n^{(1)}| - p_2\sum_m |K_m^{(2)}\rangle\!\rangle\langle\!\langle K_m^{(2)}| . \qquad (14)$$

Notice that a maximally entangled state writes in the notation of Eq. (11) as $\frac{1}{\sqrt{d}}|U\rangle\!\rangle$, with U unitary and $d = \dim(\mathcal{H})$. From the invariance of the trace norm $\|UAV\|_1 = \|A\|_1$ for arbitrary unitary operators U and V [12], one obtains the following upper bound for the minimal error probability

$$p_E \le \frac{1}{2}\left(1 - \frac{1}{d}\|\Delta\|_1\right) . \qquad (15)$$

Exploiting unitarily invariance and the polar decomposition of ξ^τ as $\xi^\tau = UP$ with U unitary and P positive, the maximum in Eq. (13) can be searched for positive operators P with $\mathrm{Tr}[P^2]=1$, namely

$$p_E = \frac{1}{2}\left(1 - \max_{P\geq 0\,,\,\mathrm{Tr}[P^2]=1} \|I\otimes P\Delta I\otimes P\|_1\right) \ . \quad (16)$$

This expression is very suitable for numerical evaluation. Moreover, the rank of P that achieves the maximum gives directly information about the usefulness of entanglement. There is no need of entanglement for the optimal discrimination if and only if the maximum in Eq. (13) can be achieved by a rank-one operator P.

The minimal error probability can be evaluated when the quantum operations can be realized from the same set of orthogonal unitaries (namely $\{U_n\}$ with $\mathrm{Tr}[U_m^\dagger U_n] = d\delta_{n,m}$) as random unitary transformations [15]. In this case one has

$$\mathcal{E}_i(\rho) = \sum_n q_n^{(i)} U_n \rho U_n^\dagger \ , \qquad \sum_n q_n^{(i)} = 1 \quad (17)$$

and hence $\Delta = \sum_n r_n |U_n\rangle\!\rangle\langle\!\langle U_n|$, with $r_n = p_1 q_n^{(1)} - p_2 q_n^{(2)}$. The operator Δ is diagonal on maximally entangled states with eigenvalues dr_n, and the bound in Eq. (15) then writes $p_E \leq \frac{1}{2}(1-\sum_n |r_n|)$. On the other hand, one has

$$\begin{aligned}&\max_{|\psi\rangle\in\mathcal{H}\otimes\mathcal{H}} \left\| \sum_n r_n (U_n\otimes I)|\psi\rangle\langle\psi|(U_n^\dagger\otimes I)\right\|_1 \\ &\leq \sum_n |r_n| \max_{|\psi\rangle} \left\|(U_n\otimes I)|\psi\rangle\langle\psi|(U_n^\dagger\otimes I)\right\|_1 \\ &= \sum_n |r_n| \ . \end{aligned} \quad (18)$$

From Eq. (18) one has $p_E \geq \frac{1}{2}(1-\sum_n |r_n|)$, and together with the upper bound (15), one obtains

$$p_E = \frac{1}{2}\left(1 - \sum_n |r_n|\right) = \frac{1}{2}\left(1 - \frac{1}{d}\|\Delta\|_1\right) \ . \quad (19)$$

This result implies that in the case of Eq. (17) the minimal error probability can always be obtained by using an arbitrary maximally entangled state at the input.

Notice that by dropping the condition of orthogonality of the $\{U_n\}$, one just obtains the bounds

$$\frac{1}{2}\left(1 - \sum_n |r_n|\right) \leq p_E \leq \frac{1}{2}\left(1 - \frac{1}{d}\|\Delta\|_1\right) \ . \quad (20)$$

In the following we consider the case of discrimination of two Pauli channels for qubits, namely

$$\mathcal{E}^{(i)}(\rho) = \sum_{\alpha=0}^{3} q_\alpha^{(i)} \sigma_\alpha \rho \sigma_\alpha \ , \quad (21)$$

where $\{\sigma_0\,,\sigma_1\,,\sigma_2\,,\sigma_3\} = \{I\,,\sigma_x\,,\sigma_y\,,\sigma_z\}$ and $\sum_{\alpha=0}^{3} q_\alpha^{(i)} = 1$. In particular, we are interested to understand when the entangled-input strategy is really needed to achieve the optimal discrimination. The positive operator P in Eq. (16) can be parameterized on the computational basis as follows

$$P = \begin{pmatrix} x & z \\ z^* & y \end{pmatrix} \ , \quad (22)$$

with $x, y \geq 0$, $xy \geq |z|^2$, and $x^2+y^2+2|z|^2 = 1$. The strategy with unentangled input corresponds to the values range $x+y=1$ and $|z| = \sqrt{xy}$ such that $\mathrm{rank}(P) = 1$. The operator Δ is diagonal on the Bell basis and writes $\Delta = \sum_{\alpha=0}^{3} r_\alpha |\sigma_\alpha\rangle\!\rangle\langle\!\langle\sigma_\alpha|$, where $r_\alpha = p_1 q_\alpha^{(1)} - p_2 q_\alpha^{(2)}$. On the ordered basis $\{|00\rangle\,,|01\rangle\,,|10\rangle\,,|11\rangle\}$, one has

$$\Delta = \begin{pmatrix} a & 0 & 0 & c \\ 0 & b & d & 0 \\ 0 & d & b & 0 \\ c & 0 & 0 & a \end{pmatrix} \ , \quad (23)$$

with $a = r_0 + r_3$, $c = r_0 - r_3$, $b = r_1 + r_2$, and $d = r_1 - r_2$. The singular values of Δ are given by

$$s_i(\Delta) = \{|a \pm c|\,,|b \pm d|\} \ , \quad (24)$$

and for the previous derivation we know that the minimal error probability can be achieved by using a maximally entangled input state, with

$$p_E = \frac{1}{2}\left(1 - \frac{1}{2}\sum_{i=0}^{3} s_i(\Delta)\right) = \frac{1}{2}\left(1 - \sum_{i=0}^{3} |r_i|\right) \ . \quad (25)$$

For the strategy with unentangled input one has

$$\begin{aligned} p'_E &= \frac{1}{2}\left(1 - \max_{P'} \|I\otimes P'\,\Delta\, I\otimes P'\|_1\right) \ ; \\ P' &= \begin{pmatrix} x & \sqrt{x(1-x)}e^{i\phi} \\ \sqrt{x(1-x)}e^{-i\phi} & 1-x \end{pmatrix} \ , \\ &0 \leq x \leq 1 \ , \qquad 0 \leq \phi \leq 2\pi \ . \end{aligned} \quad (26)$$

In this case the operator $\Delta' = I \otimes P'\,\Delta\, I \otimes P'$ inside the trace norm is at most rank-two, and its nonvanishing singular values write

$$s_{1,2}(\Delta') = \frac{1}{2}\Big| a + b \pm \sqrt{[(a-b)(1-2x)]^2 + 4x(1-x)(c^2+d^2+2cd\cos(2\phi))}\Big| \ .$$

The maximum can be obtained from comparing the values of $s_1(\Delta') + s_2(\Delta')$ just for the extreme points $x = 0, 1$ and the stationary points $x = 1/2$ and $\phi = k\pi/2$ with k integer, and one has

$$p'_E = \frac{1}{2}\left(1 - M\right) \ , \quad (27)$$

where

$$
\begin{aligned}
&M = \\
&\max\left\{|a|+|b|\,,\frac{1}{2}\left(|a+b+c+d|+|a+b-c-d|\right)\,,\right.\\
&\left.\frac{1}{2}(|a+b+c-d|+|a+b-c+d|)\right\} = \\
&\max\left\{|r_0+r_3|+|r_1+r_2|\,,|r_0+r_1|+|r_2+r_3|\,,\right.\\
&\left.|r_0+r_2|+|r_1+r_3|\right\}\ ,
\end{aligned}
\tag{28}
$$

and the three cases inside the brackets corresponds to using as input state an eigenstate of σ_z, σ_x, and σ_y, respectively. From Eq. (28) one can see that entanglement is not needed as long as $M = \sum_{i=0}^{3} |r_i|$, and this happens in many situations: *i)* when the determinant $\det(\Delta) = 0$, namely at least one of the $\{r_i\}$ vanishes; *ii)* when $\det(\Delta) > 0$, so that two of the $\{r_i\}$ are strictly positive and the other are strictly negative. On the other hand, entanglement is crucial to achieve the ultimate minimal error probability when $\det(\Delta) < 0$. Among these cases, there are striking examples where the channels can be perfectly discriminated only by means of entanglement. This is the case of two channels of the form

$$
\mathcal{E}_1(\rho) = \sum_{\alpha\neq\beta} q_\alpha \sigma_\alpha \rho \sigma_\alpha\ , \qquad \mathcal{E}_2(\rho) = \sigma_\beta \rho \sigma_\beta\ , \tag{29}
$$

with $q_\alpha \neq 0$, and arbitrary a priori probability. This example can be simply understood, since the entangled-input strategy increases the dimension of the Hilbert space such that the two possible output states will have orthogonal support.

In conclusion, we considered the problem of discriminating two quantum operations with minimal error probability and showed that the use of entangled input states generally improves the discrimination. We gave a general upper bound to the minimal error probability, and the exact solution for generalized Pauli channels. In the case of qubits, we characterized in a simple way the Pauli channels where the use of entanglement definitely outperforms the scheme with unentangled input. We hope that our results will stimulate further research on the discrimination of quantum operations.

Acknowledgments. Stimulating discussions with G. M. D'Ariano are acknowledged. This work has been sponsored by INFM through the project PRA-2002-CLON.

[1] W. K. Wootters, Phys. Rev. D **23**, 357 (1981); S. L. Braunstein and C. M. Caves, Phys. Rev. Lett. **72**, 3439 (1994).

[2] A. Gilchrist, N. K. Langford, and M. A. Nielsen, quant-ph/0408063; V. P. Belavkin, G. M. D'Ariano, and M. Raginsky, quant-ph/0408159.

[3] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).

[4] For a recent review, see J. Bergou, U. Herzog, and M. Hillery, *Quantum state estimation*, Lecture Notes in Physics Vol. 649 (Springer, Berlin, 2004), p. 417; A. Chefles, *ibid.*, p. 467.

[5] B. Huttner, A. Muller, J. D. Gautier, H. Zbinden, and N. Gisin, Phys. Rev. A **54**, 3783 (1996); S. M. Barnett and E. Riis, J. Mod. Opt. **44**, 1061 (1997); R. B. M. Clarke, A. Chefles, S. M. Barnett, and E. Riis, Phys Rev A. **63**, 040305(R) (2001); R. B. M. Clarke, V. M. Kendon, A. Chefles, S. M. Barnett, E. Riis, and M. Sasaki, Phys. Rev. A **64**, 012303 (2001); M. Mohseni, A. M. Steinberg, and J. A. Bergou, Phys. Rev. Lett. **93**, 200403 (2004).

[6] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987); D. Dieks, Phys. Lett. A **126**, 303 (1988); A. Peres, Phys. Lett. A **128**, 19 (1988); G. Jaeger and A. Shimony, Phys. Lett. A **197**, 83 (1995); A. Chefles, Phys. Lett. A **239**, 339 (1998).

[7] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000); S. Virmani, M. F. Sacchi, M. B. Plenio, and D. Markham, Phys. Lett. A **288**, 62 (2001); Y.-X. Chen and D. Yang, Phys. Rev. A **64**, 064303 (2001); **65**, 022320 (2002); Z. Ji, H. Cao, and M. Ying, Phys. Rev. A **71**, 032323 (2005).

[8] A. M. Childs, J. Preskill, and J. Renes, J. Mod. Opt. **47**, 155 (2000); A. Acín, Phys. Rev. Lett. **87**, 177901 (2001); G. M. D'Ariano, P. Lo Presti, and M. G. A. Paris, Phys. Rev. Lett. **87**, 270404 (2001).

[9] V. I. Paulsen, *Completely Bounded Maps and Dilations* (Longman Scientific and Technical, New York, 1986).

[10] D. Aharonov, A. Kitaev, and N. Nisan, in "Proceedings of the 30th Annual ACM Symposium on Theory of Computation (STOC)", p. 20, 1997.

[11] A. S. Holevo and R. F. Werner, Phys. Rev. A **63**, 032312 (2001).

[12] See, for example, R. Bhatia, *Matrix Analysis*, Springer Graduate Texts in Mathematics Vol. 169 (Springer, New York, 1996).

[13] K. Kraus, *States, Effects and Operations*, Lecture Notes in Physics Vol. 190 (Springer, Berlin, 1983).

[14] G. M. D'Ariano, P. Lo Presti and M. F. Sacchi, Phys. Lett. A. **272**, 32 (2000).

[15] This generalizes Pauli channels in arbitrary dimension. An example of such a set is operators of the form $X^k Z^l$ where X and Z act on the basis states $|0\rangle, ..., |d-1\rangle$ as $X|j\rangle = |j \oplus 1\rangle$ and $Z|j\rangle = e^{2\pi i j/d}|j\rangle$, with $\oplus$ denoting addition modulo d. Other examples and general theory can be found in Ref. [16].

[16] A. Klappenecker and M. Roetteler, IEEE Trans. Inf. Theory **48**, 2392 (2002).